PCT/JP2004/008636

日本国特許庁
JAPAN PATENT OFFICE

27.08.2004

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日
Date of Application: ２００３年　７月１８日

出願番号
Application Number: 特願２００３－１９９５１４

[ST. 10/C]: [ＪＰ２００３－１９９５１４]

出願人
Applicant(s): グローバルフレンドシップ株式会社

２００４年１０月　７日

特許庁長官
Commissioner,
Japan Patent Office

小川洋

出証番号　出証特２００４－３０９０１８３

【書類名】　特許願
【整理番号】　GFS0024
【あて先】　特許庁長官　殿
【国際特許分類】　G06F 12/00
【発明者】
　【住所又は居所】　東京都渋谷区幡ヶ谷１丁目１１番１３号－５０６
　【氏名】　保倉　豊
【特許出願人】
　【識別番号】　500401453
　【氏名又は名称】　グローバルフレンドシップ株式会社
【代理人】
　【識別番号】　100104341
　【弁理士】
　【氏名又は名称】　関　正治
【手数料の表示】
　【予納台帳番号】　041232
　【納付金額】　21,000円
【提出物件の目録】
　【物件名】　明細書　1
　【物件名】　図面　1
　【物件名】　要約書　1
【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　電子情報管理システム

【特許請求の範囲】

【請求項１】　本人認証を行って本人に帰属する電子情報を提示する電子計算機システムであって、演算装置と複数のファイルを備え、該演算装置が本人認証情報の電子情報と本人帰属電子情報のそれぞれを分割して別々のファイルに格納し、さらに格納情報を公開情報ファイルに保存して、また前記演算装置は、電子情報提示の要求を受け取ると公開情報ファイルから格納情報を引き出し該格納情報に従って前記ファイルから本人認証情報の電子情報を集合して本人認証情報を復元し、該復元した本人認証情報と入力された本人認証情報と対比して本人認証し、該本人認証に合格したときに初めて各ファイルから本人帰属電子情報を集合し復元して提示することを特徴とする電子情報管理システム。

【請求項２】　前記本人認証電子情報および本人帰属電子情報の分割は、該電子情報を指定するビット位置で切って複数の小さな情報エレメントに分け、秘密分散法アルゴリズムを用いて指定した順番に該複数の情報エレメントを置き換え、さらに指定数に分割し電子情報ブロックとして別々のファイルに格納するもので、前記本人認証電子情報および本人帰属電子情報の復元は、前記電子情報ブロックを格納したファイルから対象の電子情報に係る電子情報ブロックを集合して、前記指定された順番に基づいて情報エレメントを元の順に並べ替え、相互に接続して元の電子情報に復元するものであることを特徴とする請求項１記載の電子情報管理システム。

【請求項３】　前記本人認証電子情報および本人帰属電子情報の分割において、前記電子情報または前記電子情報ブロックは情報圧縮を施すことを特徴とする請求項２記載の電子情報管理システム。

【請求項４】　前記本人認証情報を複数種類格納して、本人帰属情報の重要度に応じて確認するべき本人認証情報の種類および組み合わせを公開情報ファイルに格納したリストから指定することができることを特徴とする請求項１から３のいずれかに記載の電子情報管理システム。

【請求項５】　前記電子情報はｎ個に分割したものを重複して別々のファイ

ルに格納することにより１個以上ｋ個（ただしｋは（ｎ－１）＞ｋ＞＝１の関係を満たす整数）のファイルが欠損しても電子情報が復元できるようにしたことを特徴とする請求項１から４のいずれかに記載の電子情報管理システム。

【請求項６】　前記本人帰属電子情報の提示要求および提示は、通信端末装置を介して行うことを特徴とする請求項１から５のいずれかに記載の電子情報管理システム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、記憶した電子情報を権原あるユーザ以外に提供しないようにした電子情報管理システムに関する。

【０００２】

【従来の技術】

銀行が管理する顧客の預金や融資などの金融情報、医療機関における患者の診断表などの医療情報、証券会社などにおける顧客の資産情報、戸籍や住民票などの行政情報、あるいは企業内部情報や著作権情報など、個人のプライバシーに関する情報や個人に帰属すべき情報を情報管理システムの電子計算機の記憶装置に格納しておいて、必要に応じて、インターネットなどのコンピュータネットワークを介して引き出して利用する形態が発展しつつある。このような情報管理システムは個人情報と無関係の多数の者が利用するので、対象とする情報に係る権原あるユーザしか個人情報を引き出せないようにする必要がある。

【０００３】

従来、図６に例示するように、多数の顧客の端末装置がネットワーク通信路を介して情報管理コンピュータに繋がるシステムでは、まず端末装置と情報管理装置の間で整合しているかを検査する。端末装置がシステムにおいて加盟者のひとつであることが確認されると初めて相互の接続が認められる。さらに端末装置を操る者が会員として登録された者であることを識別番号ＩＤと暗証番号ＰＩＮで確認できてから、初めて記憶装置に格納された電子情報を引き出して端末装置に送信する。

このように、コンピュータネットワーク上の電子情報を保護するため本人認証を行って合格した者にのみ情報を供与する方法を採用することが多かった。

【０００４】

なお、認証とは、本人を確認し、その本人に帰属する権限を付与する仕組みである。現状における認証では、事前に登録された本人を確認するための情報を丸ごと運用管理し、認証要求者がその事前に入力された本人確認情報と同じか、一定の振れ幅の範囲に収まる認証情報を提供できたときに、システム側が本人と見なしてその入力者に対し特定の権限を認可したり帰属情報を開示する。

たとえば、特許文献１には、銀行が管理している顧客の属性や履歴に関する顧客帰属情報を格納してネットワークを介して顧客パソコンに提供する金融情報提供システムが開示されている。

【０００５】

また、コンピュータネットワークでは、愉快犯やクラッカー達がネットワーク通信路を介してコンピュータシステムに侵入し、コンピュータシステム自体やオペレーションシステムなどの部分に対して、巧妙に不正を働きそのシステムが管理している情報を入手したり改変を加えたりすることを容易に防ぐことができない。

このため、従来の本人認証により保護する方法によっても、権原のない第三者が、たとえば、本人認証用情報を盗み出して本人になりすましたり、本人帰属情報などを丸ごと盗み出して利用されたりする危険があった。

特許文献２には、このような危険を少しでも小さくする技術として、認証情報を分割し、分割されたユーザ認証情報の構成要素のうち一方をシステム側にまた他方をユーザ側の登録情報として割り当て、本人認証するときに分散管理された電子情報を集めて元のユーザ認証情報を生成復元して本人認証するようにした認証システムを開示している。

【０００６】

【特許文献１】

特開２００２－００７６９７号公報

【特許文献２】

特開２００２－３１２３１７号公報

【０００７】

【発明が解決しようとする課題】

そこで、本発明が解決しようとする課題は、利便性を維持しながら格納した情報の安全性を高めた情報の運用管理システムを提供することである。

【０００８】

【課題を解決するための手段】

上記課題を解決するため、本発明の電子情報管理システムは、本人認証を行って本人に帰属する電子情報を提示するシステムであって、本人認証情報の電子情報と本人帰属電子情報のそれぞれを分割して別々のファイルに格納し、格納情報を公開情報ファイルに保存して、電子情報提示の要求があったときには、演算装置が公開情報ファイルから引き出した格納情報に基づいてファイルから本人認証情報の電子情報を集合して本人認証情報を復元して入力された本人認証情報と対比して本人確認し、本人認証に合格したときに初めて各ファイルから本人帰属電子情報を集合して復元し提示することを特徴とする。

【０００９】

本発明の電子情報管理システムは、必要とされる電子情報が分割され複数のファイルに分離して格納されているので、無権限者がアクセスしても復元に必要な電子情報を落ちなく集めることが難しい。したがって、本人になりすますための認証情報が窃取される危険が小さい。また、本人認証に合格しない限り本人帰属情報に係る電子情報の集合と復元をしないようにすれば、本人帰属情報を摂取することがさらに格段に難しくなり、情報の安全性が高い。

【００１０】

なお、本人認証電子情報および本人帰属電子情報の分割は、指定したビット位置で電子情報を切って複数の小さな情報エレメントに分け、秘密分散法アルゴリズムを用いてこの複数の情報エレメントを指定した順番に置き換え、さらに順番が置き換えられた全体を指定数に分割し電子情報ブロックとして別々のファイルに格納するものであることが好ましい。また、本人認証電子情報および本人帰属電子情報の復元は、電子情報ブロックを格納したファイルから対象の情報に係る

電子情報ブロックを集合して、分割時に指定した順番に基づいて情報エレメントを元の順に並べ替え、相互に接続して元の電子情報に復元することが好ましい。

【００１１】

この明細書において、秘密分散法（Secret Sharing Scheme）とは、秘密共有法の一種で、ある秘密sをn個に分散し、そのうちのk個以上を集めるとsが完全に復元できるが、(k-1)個では情報が得られない性質を持つ基本的な理論と、これに類似した各種の理論を含む。典型的な手法では、(k-1)個の情報が洩れても秘密sは安全であり、また、(n-k)個の情報を紛失してもsの復元が可能である。秘密分散法アルゴリズムとは、秘密分散法を実際に実施するための論理であって、電子計算機に実施させるためにはプログラムの形で利用する。

【００１２】

本発明の電子情報管理システムは、さらに、本人認証電子情報および本人帰属電子情報の分割において、電子情報または電子情報ブロックに情報圧縮を施すことが好ましい。

このような電子割符技術を利用することにより、いろいろな手法による電子情報の漏洩は阻止でき、情報の保護はさらに一段と確実になる。

また、本人認証情報を複数種類格納して、本人帰属情報の重要度に応じて確認するべき本人認証情報の種類および組み合わせを指定するようにすることが好ましい。

【００１３】

電子情報を複数に分割して生成した電子情報ブロックは別々のファイルに重複して格納するようにしてもよい。重複格納することにより、一部のファイルが欠損しても電子情報を復元することができる。

なお、本発明の電子情報管理システムにおいて、本人帰属電子情報の提示要求および提示は、パソコン、ＰＤＡ、携帯電話など、通信端末装置を介して行うことができる。

また、本発明で採用されたような、電子情報を分割し分離したファイルにそれぞれ格納するという技術的思想は、電子計算機システムの記憶装置に格納する電子情報を保護するためにも活用することができることはいうまでもない。

【００１４】

【発明の実施の形態】

以下、図面を参照して本発明の電子情報管理システムを実施例に基づいて詳細に説明する。

本実施例の電子情報管理システムは、図６に示したと同じく、通信ネットワークを介してユーザの通信端末機に接続され、ユーザのために蓄積された各種の本人帰属情報を保管する計算機システムである。

本人帰属情報としては、病院が運用する電子情報管理システムとした医療情報や、銀行や証券会社で運用する情報管理システムにおける資産情報などがある。また、地方自治体が行政に伴い発生し蓄積する各種行政情報も対象とすることができる。これら以外にも、個人のプライバシーに属して他人に開示したくない情報がたくさんある。これら個人に帰属すべき情報を随意受託して保管する機関を設けて本実施例の電子情報管理システムとして運営してもよい。また、特定のプロバイダの有する電子計算機システムに個人の電子情報を預託して電子情報管理システムとして利用することもできる。

【００１５】

本実施例の電子情報管理システムは、本人認証データを分割してその分割片を分散して保管し、さらに階層を異にして本人帰属情報データを分割して分割片を分散して保管するところに特徴がある。常時はこれら利用可能な情報が１カ所にまとまって存在しないから、第三者の攻撃に対して耐性が強く、安全性が高い。

特に、いわゆる電子割符技術を活用して、電子情報を細分して情報エレメントとし、これをランダムに配列し直してから複数の情報ブロックに分け、それぞれの情報ブロックをばらばらに保管するようにした場合は、権原無き第三者が一部の情報ブロックを窃取することに成功しても何のコンテンツも知ることができない。

【００１６】

また、たとえ関連する全ての情報ブロックを収集することに成功しても分割や配列替えなどの情報を持たなければ意味を有する情報に復元することができないので安全である。

さらに、細分する前の電子情報や分割して生成した情報ブロックについて信号圧縮処理を施す電子割符技術を用いたときは、極めて安全に電子情報の管理をすることができる。

また、始めに本人認証データの分割片を集合して復元した情報と入力された本人認証情報と照合し、照合結果が良好であるときに初めて本人帰属情報データについて分割片を集合して復元するようにするので、本人帰属情報が常時は意味を取ることが困難な状態で保管されていて、最も保護したい本人帰属情報の漏洩を高度に防止することができる。

【００１７】

図１は、本実施例のシステムにおいて、記憶装置に電子情報を格納するためのフォーマットの例を示すブロック図である。また、図２と図３は、電子情報を格納する手順例を説明するフロー図、図４は自己に帰属する情報を取り出すときの手順を説明するフロー図である。

電子情報管理システムは、ユーザを会員として登録すると、個々のユーザについてそれぞれ固有のフォルダ１を記憶装置内に生成する。なお、フォルダ１はランダムファイル形式など、予め大きさや位置を固定して指定しておかずに、必要に応じて拡張性を持たせた形式のものであることが好ましい。

【００１８】

フォルダ１の中には複数のファイルが生成される。

フォルダ内に設定されるファイルには、会員登録の時に決め、また会員の要請により随時変更した、会員の識別番号ＩＤと暗証番号ＰＷを格納するユーザ認証ファイルと、システムと端末接続機器の整合性を判定するための情報を記録した機器整合性検査用ファイルとを一緒にした接続用ファイル１１がある。

あるユーザが自身の端末装置を電子情報管理システムに接続するためには、まず、端末装置がシステムに承認を受けて登録されたものであるかの検査に合格しなければならない。この機器整合性検査に合格して端末装置とシステムが接続された後に、ユーザが識別番号ＩＤと暗証番号ＰＷを入力する。これらの情報はシステムに送信され、システムが入力された識別番号ＩＤや暗証番号ＰＷと、ユーザ認証ファイルに格納されていた識別番号ＩＤと暗証番号ＰＷとを比較して同一

性を検査し、この検査に合格したときに始めてユーザの端末装置を受け入れて、システムの計算機に対するアクセスを認める。

【００１９】

フォルダ１の中には、分割された個人情報の分割片を格納する個人情報ファイル１２ａ，１２ｂが設けられる。個人情報ファイルの個数はいくつであってもよいが、図１には説明を簡単にするため２個のケースについて表示してある。

個人情報ファイル１２ａ，１２ｂの中には、それぞれ公開情報ファイル２１ａ，２１ｂ、認証情報ファイル２２ａ，２２ｂ、個人帰属情報ファイル２３ａ，２３ｂが含まれる。

【００２０】

公開情報ファイル２１ａ，２１ｂは、多数のファイルから個人情報ファイル１２ａ，１２ｂを選択するために使用する指標値を特に暗号処理を施さないで格納するヘッダーファイルともいうべきもので、情報復元に必要なファイルを簡単に収集できるようにしてある。

認証情報ファイル２２ａ，２２ｂは、個人帰属情報にアクセスする者の権原を確認するための認証情報を格納するものである。本人認証は、暗証番号、暗号鍵、署名、証明書、署名の動的入力値、指紋、掌紋、声紋、虹彩紋、容貌の特徴、その他の生物学的特徴、さらにＩＣカードなどの所有物により真正を証明する方法など、各種のもので行うことができる。

【００２１】

これら認証情報を複数種類格納しておいて、引き出そうとする電子情報によって認証手段を選択するようにすることもできる。また、重要な対象情報など厳格な本人認証を要求する場合は、予め決めた２種以上の認証に適合しなければ読み出せないようにしても良い。

認証情報は、いわゆる電子割符技術を用いて、複数に分割し分割片３１ａ，３１ｂを異なる複数のファイル２２ａ，２２ｂに格納し、必要なときに分割片を全て収集して逆の手順で元の情報に復元して利用するようにすると、格納された電子情報の安全性が確保できる。

【００２２】

また、個人帰属情報ファイル２３ａ，２３ｂは、上に述べたような個人帰属情報を格納する。個人帰属情報も、電子割符技術を用いて、複数に分割し分割片３２ａ，３２ｂを異なる複数のファイル２３ａ，２３ｂに格納し、必要なときに分割片を全て収集して逆の手順で元の情報に復元して利用する。

【００２３】

電子情報管理システムを利用するためには、予めシステムに電子情報を格納しておく必要がある。システムの用途によっては格納すべき電子情報をユーザ自身が入力するのではなく、病院や金融機関、あるいは役所などが生成して蓄積しても良い。ここでは、ユーザ自身が電子情報を預託しておく場合について説明する。

【００２４】

フォルダ１の中には、権原情報ファイル１３が設けられる。

個人帰属情報は当該個人またはその個人に認可された特定の人しか引き出しを認めない。このため、引き出しをしようとしている人物が個人帰属情報の引き出しを認める人物であることを本人認証手段で確認する。

個人帰属情報ごとにどの本人認証手段を利用するかについて明確にした対照表は、権原情報ファイル１３に格納される。

なお、権原情報は電子割符処理して、個人情報ファイル１２の中に分散して格納するようにしても良い。

【００２５】

図２は、認証情報を格納する手順を例示したものである。

認証情報はユーザの端末装置あるいは登録に使うコンピュータを介して電子情報管理システムに入力される（Ｓ１１）。電子情報管理システムは認証情報を入力すると、指定したビット位置で電子情報を切って複数の小さな情報エレメントに分け、生成した複数の情報エレメントを指定した順番に置き換える（Ｓ１２）。さらに順番が置き換えられた全体を指定数に分割し（Ｓ１３）、認証情報の電子情報ブロック３１ａ，３１ｂ，・・・として別々のファイル２１ａ，２１ｂ，・・・に格納する（Ｓ１４）。

認証情報の入力装置は、それぞれの認証情報の性格に従って特定のものが必要

とされるので、使用する認証方法に従って準備する必要がある。

【００２６】

図３は、電子化した個人帰属情報を格納する手順を例示したものである。

個人帰属情報はユーザの端末装置あるいはシステムのコンピュータ入力装置を介して電子情報管理システムに入力される（Ｓ２１）。電子情報管理システムは個人帰属情報を入力すると、個人帰属情報の電子情報を指定位置で切って複数の小さな情報エレメントに分け、生成した情報エレメントを指定した順番に置き換える（Ｓ２２）。さらに順番が置き換えられた全体を指定数に分割し電子情報ブロック３２ａ，３２ｂ，・・・とし（Ｓ２３）、分割された個人帰属情報の電子情報ブロック３２ａ，３２ｂ，・・・は別々の個人帰属情報ファイル２２ａ，２２ｂ，・・・に格納する（Ｓ２４）。

【００２７】

なお、これら認証情報や個人帰属情報は信号圧縮技術を用いてさらに安全性を向上させても良い。

さらに、個人帰属情報は当該個人またはその個人に認可された特定の人しか引き出しを認めないため、個人帰属情報を入力したときに、その情報の性格によって使用する認証方法を予め指定し、その結果を権原情報ファイル１３に記録する（Ｓ２５）。

【００２８】

図４は、個人帰属情報を引き出すときの手順を説明するものである。

ユーザが自身の個人帰属情報を引き出しを求めてきたときは、まずそのユーザが接続する端末装置について、予め機器整合性検査用ファイルに格納されていた情報に基づいて当該端末装置が電子情報管理システムに承認を受けて登録されたものであるか否かを確認する機器整合性検査を行う（Ｓ３１）。

検査に合格しない場合は端末装置の接続を拒絶する（Ｓ３９）。

【００２９】

機器整合性検査に合格して端末装置とシステムが接続された後に、ユーザの適正を確認する（Ｓ３２）。ユーザが識別番号ＩＤと暗証番号ＰＷを入力すると、システムがこれらの情報を入力して、ユーザ認証ファイルに格納されていた識別

番号および暗証番号と比較して同一性を検査し、この検査に合格したときに初めてユーザの端末装置を受け入れて、システムの計算機に対するアクセスを認める。

ユーザ端末を受け入れたときには、ユーザが求める個人帰属情報を開示するために必要とされる認証方法を権原情報ファイル１３から読み出して表示する（Ｓ３３）。

【００３０】

ユーザは、指定された認証情報を対応する入力装置から入力する。システムは入力認証情報を取り込むと（Ｓ３４）、認証情報ファイル２２ａ，２２ｂから予め格納しておいた該当認証情報の電子情報ブロック３１ａ，３１ｂを収集して、格納時に分割して分散させた手順の逆の手順を踏んで、情報エレメントを正しい順に並べ直して元の情報を復元する（Ｓ３５）。こうして復元した元の認証情報と入力された認証情報を比較して真正か否かを判断し（Ｓ３６）、入力された認証情報が真正でなければそれ以上のアクセスを拒絶する（Ｓ３９）。

【００３１】

入力された認証情報が復元した基準の認証情報と一致したときは、続いて、個人帰属情報ファイル２３ａ，２３ｂから格納された目的の個人帰属情報の電子情報ブロック３２ａ，３２ｂを収集して、格納時に分割して分散させた手順の逆の手順を踏んで、情報エレメントを正しい順に並べ直して元の情報を復元する（Ｓ３７）。こうして復元した電子情報をユーザの端末装置に伝送して（Ｓ３８）、ユーザの要請に応える。

【００３２】

本実施例の電子情報管理システムでは、常時は肝心の電子情報が分割され複数のファイルに分散して格納されているので、外部から権原のない第三者が攻撃してきても情報コンテンツを盗むことが極めて困難である。特に電子割り符技術を用いて分割した場合は、極めて高い安全度を確保することができる。

また、個人帰属情報をユーザに提供するときにも、照合に必要な認証情報のみを復元し、認証情報の照合に合格したときに初めて目的の個人帰属情報のみを復元するなど、最小限必要な電子情報のみが復元される伝送されるので、システム

内や通信路内の情報漏洩の危険度も低い。

【００３３】

なお、こうして分散化された個人情報ファイル１２ａ，１２ｂ自体をユーザに引き渡して、ユーザ自身が個人帰属情報を管理するようにしても良い。あるいは、ユーザ自身が所有する電子計算機に上記説明の手順を実行させる情報管理ソフトウエアを備えて、上記の手法で個人帰属情報を分割し複数の個人情報ファイルに格納して情報管理するようにしても良い。

【００３４】

また、電子情報の格納時に、必要に応じてファイルに欠損があったときにも正しく情報復元ができる方式を選択できるようにすることもできる。

図５は、その方策の例としてＮ個のファイルに分割電子情報を重複して分配する（Ｎ－１）方式の説明をする図面である。

元の情報を３個の分割情報①，②，③に分割し３個のファイルＡ，Ｂ，Ｃに格納する場合に、各ファイルに異なる分割情報を２個ずつ格納しておく。すると、１個のファイル、たとえばファイルＡが損傷を受けたり欠落したりして電子情報の回収ができなくなっても、残った２個のファイルＢ，Ｃで元の情報を完全に復元することができる。

【００３５】

上記説明は、３個のファイルを使用した例を示したが、任意の数Ｎのファイルを使う場合にも２個ずつ重複して格納すれば、同じように任意の１個のファイルが欠損しても、残りの（Ｎ－１）個のファイルから元の情報を完全に復元することができる。

このような（Ｎ－１）方式を利用することによって、情報の安全性に影響を与えずに情報ファイルに欠損があっても簡単にリカバリーができるようになる。

【００３６】

また、ｎ個に分割した分割情報の重複数を増やしてＮ個のファイルに格納することによって、任意の最大ｋ個のファイルが欠損しても回復できるようにすることもできる。ここでｋは、（ｎ－１）＞ｋ≧１の関係を満たす整数である。このような手法を（Ｎ－ｋ）方式と呼んでいる。

【００３７】

【発明の効果】

以上詳細に説明した通り、本発明の電子情報管理システムによれば、自己に帰属する電子情報についても他人からの攻撃に対して安全な管理を簡単に実現させることができる。

【図面の簡単な説明】

【図１】

本発明の電子情報管理システムの１実施例において、記憶装置に電子情報を格納するためのフォーマットの例を示すブロック図である。

【図２】

本実施例における認証情報を格納する手順を例示した流れ図である。

【図３】

本実施例における電子化した個人帰属情報を格納する手順を例示した流れ図である。

【図４】

本実施例における個人帰属情報を引き出すときの手順を説明する流れ図である。

【図５】

本実施例に用いるＮ個のファイルに分割電子情報を重複して分配するＮ－１方式の説明をする図面である。

【図６】

多数の端末装置がネットワーク通信路を介して情報管理コンピュータに繋がる電子情報管理システムを示すブロック図である。

【符号の説明】

１　会員用フォルダ

１１　接続用ファイル

１２ａ，１２ｂ　個人情報ファイル

１３　権原情報ファイル

２１ａ，２１ｂ　公開情報ファイル

２２ａ，２２ｂ　認証情報ファイル

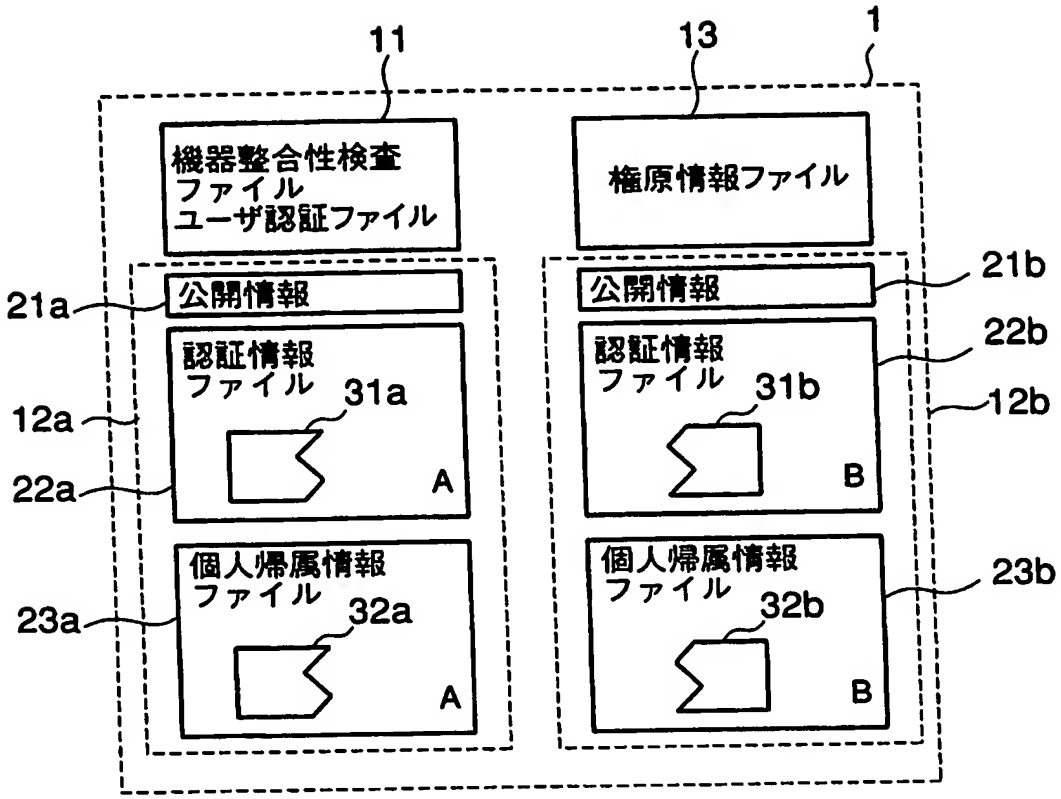
２３ａ，２３ｂ　個人帰属情報ファイル

３１ａ，３１ｂ　認証情報の電子情報ブロック

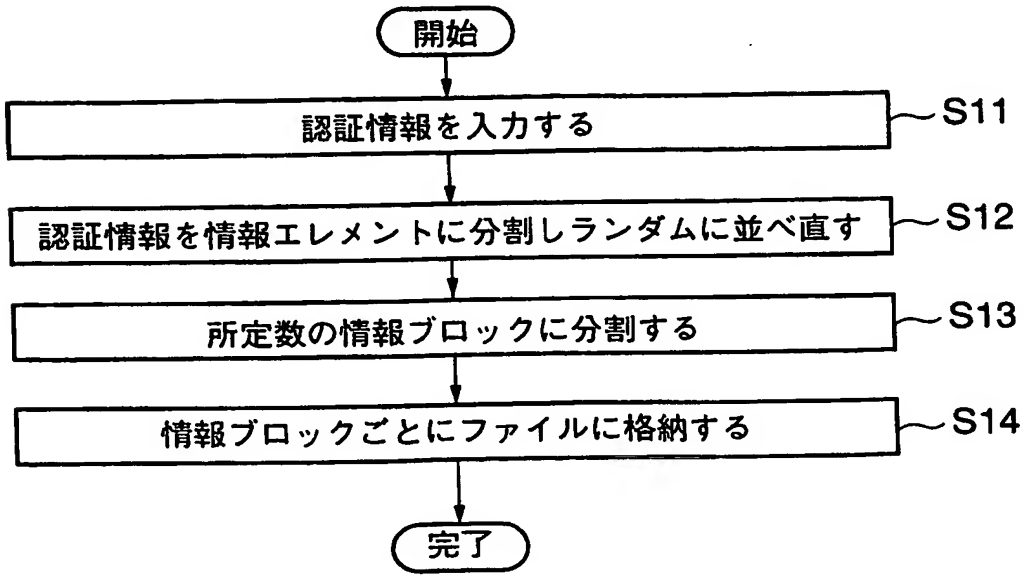
３２ａ，３２ｂ　個人帰属情報の電子情報ブロック

【書類名】　図面

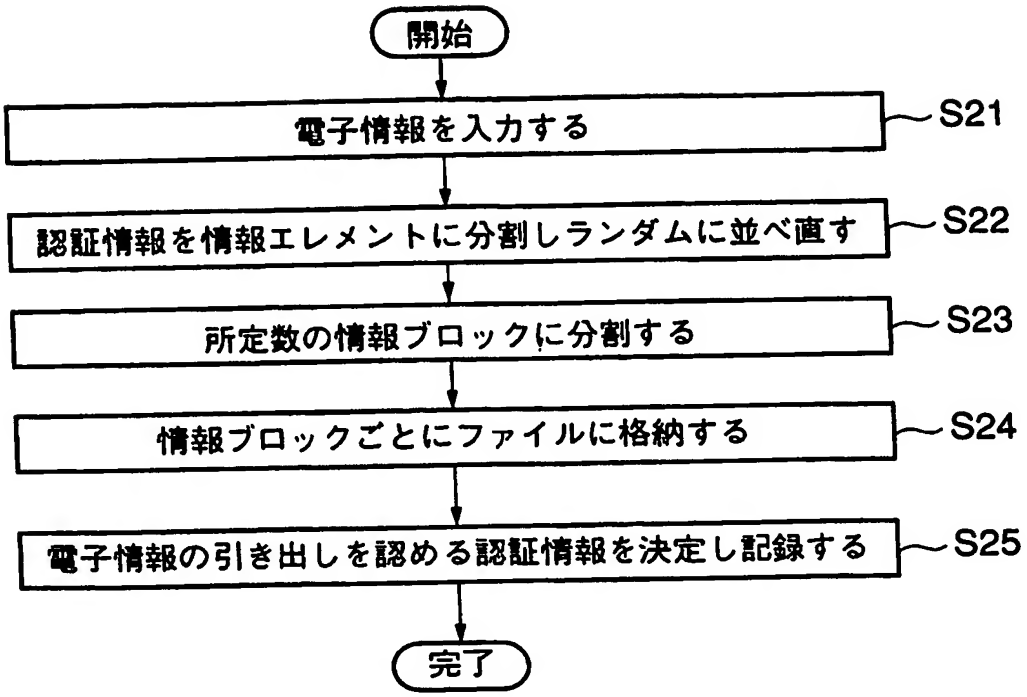
【図１】


11
13
1
機器整合性検査
ファイル
ユーザ認証ファイル
権原情報ファイル
21a
公開情報
21b
公開情報
認証情報
ファイル
31a
12a
22a
A
22b
認証情報
ファイル
31b
12b
B
個人帰属情報
ファイル
32a
23a
A
個人帰属情報
ファイル
32b
23b
B

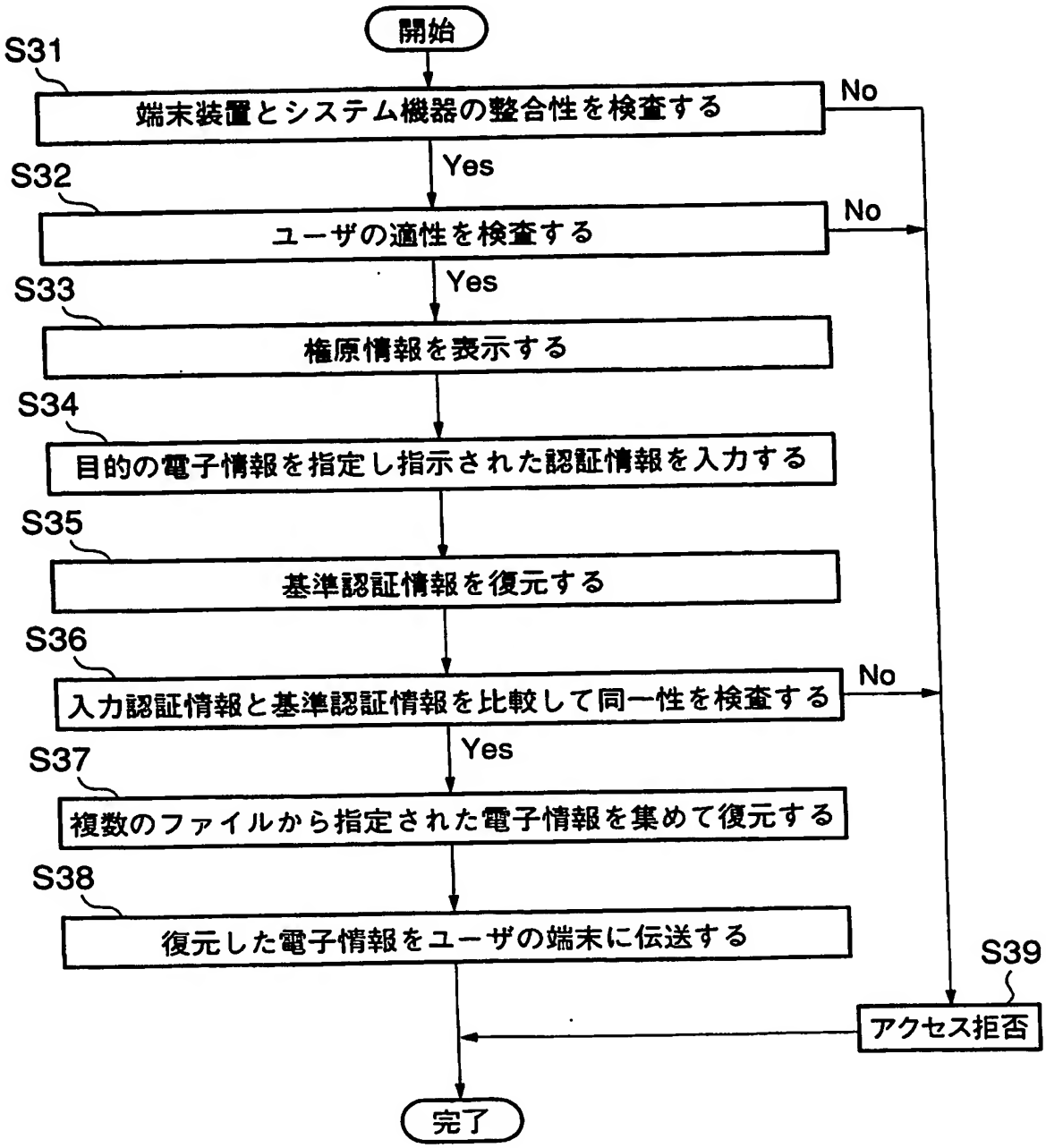
【図２】


開始
認証情報を入力する
S11
認証情報を情報エレメントに分割しランダムに並べ直す
S12
所定数の情報ブロックに分割する
S13
情報ブロックごとにファイルに格納する
S14
完了

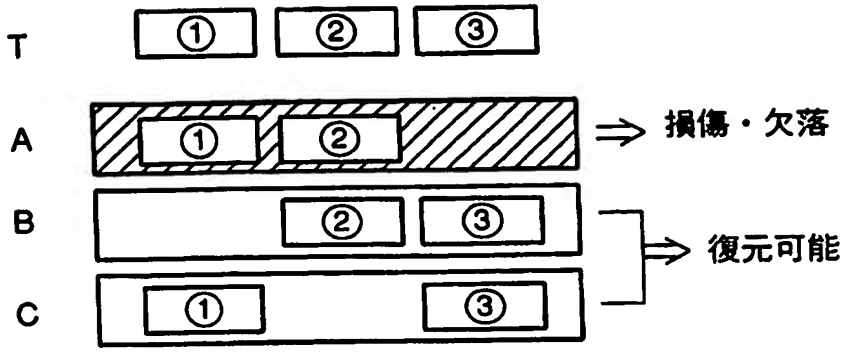
【図３】


開始
電子情報を入力する
S21
認証情報を情報エレメントに分割しランダムに並べ直す
S22
所定数の情報ブロックに分割する
S23
情報ブロックごとにファイルに格納する
S24
電子情報の引き出しを認める認証情報を決定し記録する
S25
完了

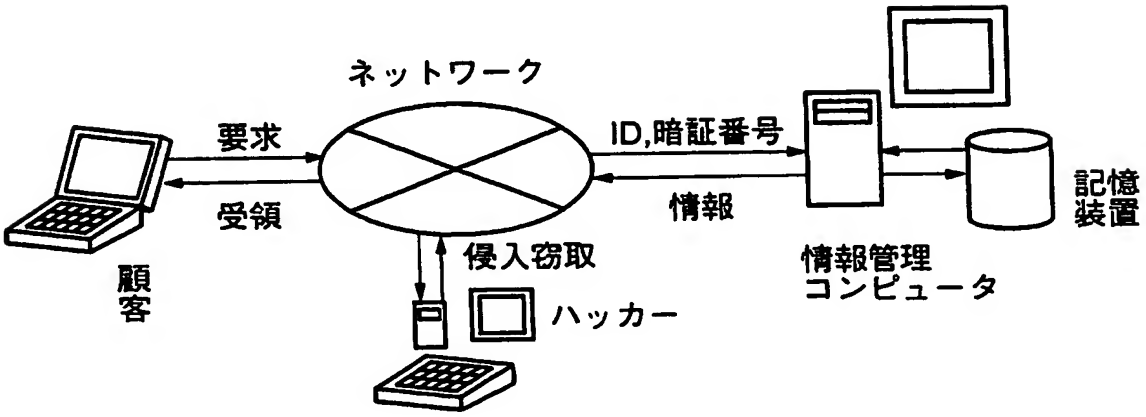
【図４】


開始
S31
端末装置とシステム機器の整合性を検査する
No
Yes
S32
ユーザの適性を検査する
No
Yes
S33
権原情報を表示する
S34
目的の電子情報を指定し指示された認証情報を入力する
S35
基準認証情報を復元する
S36
入力認証情報と基準認証情報を比較して同一性を検査する
No
Yes
S37
複数のファイルから指定された電子情報を集めて復元する
S38
復元した電子情報をユーザの端末に伝送する
S39
アクセス拒否
完了

【図５】


T
①
②
③
A
①
②
⇒ 損傷・欠落
B
②
③
⇒ 復元可能
C
①
③

【図６】


ネットワーク
要求
受領
ID,暗証番号
情報
記憶
装置
顧
客
侵入窃取
ハッカー
情報管理
コンピュータ

【書類名】　要約書

【要約】

【課題】　格納した情報の安全性を高めた情報の運用管理システムを提供する。

【解決手段】　本人認証を行って本人に帰属する電子情報を提示する電子計算機システムであって、本人認証情報の電子情報３１と本人帰属電子情報３２のそれぞれを分割して、分割情報３１ａ，３１ｂ；３２ａ，３２ｂを別々のファイル２２ａ，２２ｂ；２３ａ，２３ｂに格納して、電子情報提示の要求があったときにはファイルから本人認証情報の電子情報３１ａ，３１ｂを集合して本人認証情報を復元して入力された本人認証情報と対比して本人確認し、本人認証に合格したときに初めて各ファイルから本人帰属電子情報３２ａ，３２ｂを集合して復元し提示する。

【選択図】　図１

認定・付加情報

特許出願の番号	特願２００３－１９９５１４
受付番号	５０３０１２００７３３
書類名	特許願
担当官	第七担当上席　００９６
作成日	平成１５年　７月２２日

＜認定情報・付加情報＞

【提出日】　平成15年 7月18日

特願２００３－１９９５１４

出願人履歴情報

識別番号　[５００４０１４５３]

１．変更年月日　２００１年　２月２３日
[変更理由]　住所変更
住　所　東京都新宿区四谷四丁目１３番地
氏　名　グローバルフレンドシップ株式会社